Bedingungen für das Online-Banking im Rahmen des 1822MOBILE-Girokontos

(gültig ab 14. September 2019)

Fassung 14. September 2019

1 Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels Online-Banking in dem von der Sparkasse angebotenen Umfang abwickeln. Zudem können sie Informationen der Sparkasse mittels Online-Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz (ZAG) und Kontoinformationsdienste gemäß § 1 Absatz 34(ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden einheitlich als „Teilnehmer"., Konto und Depot einheitlich als „Konto" bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des Online-Banking gelten die mit der Sparkasse gesondert vereinbarten Verfügungslimite. Ist keine gesonderte Vereinbarung getroffen, gilt das im Preis- und Leistungsverzeichnis bestimmte Limit. Eine Änderung dieser Limite kann der Konto-/Depotinhaber mit seiner Sparkasse gesondert vereinbaren. Bevollmächtigte können nur eine Herabsetzung vereinbaren

2 Voraussetzungen zur Nutzung des Online-Banking

(1) Der Teilnehmer kann das Online-Banking nutzen, wenn die Sparkasse ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Sparkasse gesondert vereinbarte Verfahren, mit dessen Hilfe die Sparkasse die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Sparkasse als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3) sowie Aufträge erteilen (siehe Nummer 4).

(3) Authentifizierungselemente sind

— Wissenselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer [PIN]),

— Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers nachweisen, wie die Sparkassen-Card mit TAN-Generator oder das mobile Endgerät), oder

— Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Sparkasse das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Sparkasse übermittelt.

3 Zugang zum Online-Banking

(1) Der Teilnehmer erhält Zugang zum Online-Banking der Sparkasse, wenn

— er seine individuelle Online-Kennung angibt und

— er sich unter Verwendung des oder der von der Sparkasse angeforderten Authentifizierungselemente(s) ausweist und

— keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Konto-/Depotinhabers) fordert die Sparkasse den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online-Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

(3) Online-Banking über mobile Apps

(a) Nutzung von Online-Banking über Apps
Online-Banking meint im Folgenden auch die Abwicklung von Bankgeschäften über eine hierfür von der Sparkasse oder Dritten angebotene App für mobile Endgeräte, z.B. die 1822MOBILE-App der 1822direkt beim 1822MOBILE-Girokonto.

(b) Vertragspartner für Apps zum Online-Banking
Wird die App für das Online-Banking nicht von der Sparkasse bereitgestellt, ist Vertragspartner des Teilnehmers für die Nutzung der App, der im App-Store jeweils ausgewiesene Anbieter. Bei der 1822MOBILE-App ist dies die 1822direkt, Gesellschaft der Frankfurter Sparkasse mbH. Der Nutzungsvertrag kommt durch Abruf der App und deren Installation nach den Vorgaben des jeweiligen App-Store-Betreibers zu den vom Anbieter hierfür ggf. vorgegebenen Bedingungen zustande.

(c) Besondere Bedingungen für die 1822MOBILE-App
Für die von der 1822direkt bereitgestellte 1822MOBILE-App gelten ergänzend die folgenden besonderen Bedingungen:

- Die 1822MOBILE-App ist die einzige Möglichkeit zur Eröffnung und Nutzung eines 1822MOBILE-Girokontos. Bestandskunden der Sparkasse, die andere über die 1822direkt vermittelte Leistungen nutzen, können nach Wahl der Sparkasse auch über das Kundenportal auf das 1822MOBILE-Girokonto zugreifen. Ein Anspruch hierauf besteht nicht.
- Der Teilnehmer erhält von der 1822direkt ein einfaches, nicht übertragbares, nicht unterlizenzierbares Recht zur Nutzung der 1822MOBILE-App sowie ggf. hierfür bereitgestellter Aktualisierungen während der Laufzeit des Nutzungsvertrags ausschließlich zum Zweck der Eröffnung und Nutzung eines 1822MOBILE-Girokontos sowie zur Nutzung als Zahlungsauslösedienst oder Kontoinformationsdienst für andere Konten mit den in der App hierfür vorgesehene Funktionen. Ergänzend gelten die Bedingungen für die Nutzung von Apps des jeweiligen App-Store-Betreibers.
- Die 1822MOBILE-App wird mindestens für die Laufzeit des Vertrages zwischen dem Teilnehmer und der Sparkasse über das 1822MOBILE-Girokonto bereitgestellt. Die 1822direkt ist berechtigt, die 1822MOBILE-App jederzeit in ihrer Funktionalität oder Gestaltung in neuen Versionen zu ändern, zu erweitern oder zu beschränken, solange dem Teilnehmer hiernach weiterhin die Nutzung des 1822MOBILE-Girokontos im vertraglichen vereinbarten Umfang möglich ist. Dies gilt ausnahmsweise nicht, wenn dem Teilnehmer nach der Änderung, Erweiterung oder Beschränkung die weitere Nutzung des 1822MOBILE-Girokontos unzumutbar ist.
- Für die Haftung der 1822direkt im Zusammenhang mit der 1822MOBILE-App gelten die zwischen Teilnehmer und Sparkasse im Übrigen vereinbarten Bedingungen für das Online-Banking entsprechend.

4 Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einen Auftrag (z.B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z.B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.

Die Sparkasse bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen (z.B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Sparkasse sieht eine Widerrufsmöglichkeit im Online-Banking ausdrücklich vor.

5 Bearbeitung von Aufträgen durch die Sparkasse

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z.B. Überweisung) auf der Online-Banking-Seite der Sparkasse oder im „Preis- und Leistungs-verzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Sparkasse oder im „Preis- und Leistungsverzeichnis" angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Online-Banking-Seite der Sparkasse oder „Preis- und Leistungsverzeichnis" der Sparkasse, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

(2) Die Sparkasse wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

– Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1).

– Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z.B. Wertpapierorder) liegt vor.

– Das Online-Banking-Datenformat ist eingehalten.

– Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3). Ist keine gesonderte Vereinbarung getroffen, gilt das im Preis- und Leistungsverzeichnis bestimmte Limit.

– Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen (z.B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Sparkasse die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Bedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Sparkasse den Auftrag nicht ausführen. Sie wird den Teilnehmer hierüber mittels Online-Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6 Information des Kontoinhabers über Online-Banking-Verfügungen

Die Sparkasse unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

288123 - 9263/1-3 - 21.06.2019

7 Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer, hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummer 3 und 4).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere

— nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
— nicht außerhalb des Online-Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
— nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
— nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. Sparkassen-Card mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. die Sparkassen-Card mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

– sind die Sparkassen-Card mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
– ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
– ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online-Banking (z. B. 1822MOBILE-App, Authentifizierungs-App) nicht nutzen können,
– ist die Anwendung für das Online-Banking (z. B. 1822MOBILE-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
– dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
– muss der Teilnehmer, der von der Sparkasse einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online-Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online-Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online-Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online-Banking das von der Sparkasse ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim smsTAN-Verfahren (mTAN) und QRTAN+ Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

(4) Die für das smsTAN-Verfahren (mTAN) hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online-Banking nicht mehr nutzt.

(5) Bei Nutzung des QRTAN+ Verfahrens hat der Teilnehmer zum Schutz der QRTAN+ App die unbefugte Nutzung der QRTAN+ App durch die Vergabe eines sicheren Passwortes zu verhindern.

(6) Bei Nutzung des 1822TAN+ Verfahrens hat der Teilnehmer zum Schutz der 1822MOBILE-App vor einer unbefugten Nutzung den Zugriff durch die Vergabe eines sicheren Passwortes oder durch Verwendung eines Fingerprints als persönliches Sicherheitsmerkmal zu verhindern.

(7) Es ist darauf zu achten, dass für sämtliche Zugänge verschiedene sichere Passwörter verwendet werden. Insbesondere die sicheren Passwörter für die 1822MOBILE-App und das 1822TAN+ Verfahren sowie die 1822Banking-App bzw. das 1822direkt-Kundenportal dürfen aus Sicherheitsgründen nicht übereinstimmen.

(8) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 7 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheit des Kundensystems

Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Sparkasse, insbesondere Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software, beachten.

7.4 3 Prüfung der Auftragsdaten mit von der Sparkasse angezeigten Daten

Die Sparkasse zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z.B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z.B. mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

7.4 Referenzkontovereinbarung

Für die Einhaltung der Referenzkontovereinbarung beim Tagesgeldkonto ist der Nutzer selbst verantwortlich und er trägt alle Schäden, die infolge Nichtbeachtung entstehen.

7.5 Sicherheit mobiler Endgeräte

Werden das QRTAN+ oder das 1822TAN+ Verfahren genutzt, darf das Betriebssystem des hierfür verwendeten mobilen Endgerätes nicht entgegen den Empfehlungen des Herstellers verändert werden (z.B. „Root" oder „Jailbreak"). Die Sparkasse ist berechtigt, das QRTAN+ oder das 1822TAN+ Verfahren zu sperren, wenn das Endgerät nicht gemäß den Herstellerempfehlungen eingestellt ist und bleibt.

8 Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

— den Verlust oder den Diebstahl, eines Besitzelements zur Authentifizierung (z. B. Sparkassen-Card mit TAN- Generator, mobiles Endgerät, Signaturkarte) oder
— die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest, muss der Teilnehmer die Sparkasse hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht,

— einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft Ausgeführte Aufträge

Der Kontoinhaber/Depotinhaber hat die Sparkasse unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9 Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Sparkasse sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

— den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
— seine Authentifizierungselemente zur Nut- zung des Online-Banking.

9.2 Sperre auf Veranlassung der Sparkasse

(1) Die Sparkasse darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn

— sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
— sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
— der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Sparkasse wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Sparkasse hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

Die Sparkasse wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chip-basierten Besitzelements

(1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte (z. B. Sparkassen-Card), der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in Absätzen 1 und 2 genannten Besitzelemente können dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer kann sich mit der Sparkasse in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Sparkasse kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kontoinhabers verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters

288123 - 9263/2-3 - 21.06.2019

zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Sparkasse wird den Kontoinhaber über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Sparkasse hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Sparkasse die Zugangssperre auf. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

10 Haftung

10.1 Haftung der Sparkasse bei Ausführung eines nicht autorisierten Auftrags und nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Sparkasse bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung der Authentifizierungselemente

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kontoinhaber gemäß der gesetzlichen Vorschrift des § 675v Abs. 1 BGB für den der Sparkasse hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

— es dem Teilnehmer nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder

— der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung, eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(2a) Ist der Kontoinhaber Verbraucher, verzichtet die Sparkasse auf eine Inanspruchnahme nach den unter dem vorstehenden Absatz (1) genannten gesetzlichen Bestimmungen.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

– Nummer 7.1 Absatz 2,
– Nummer 7.1 Absatz 4,
– Nummer 7.3 oder
– Nummer 8.1 Absatz 1

verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Sparkasse vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Seins (siehe Nummer 2 Absatz 3).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Sparkasse nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:

— Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

— Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2 Haftung des Konto-/Depotinhabers bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außer- halb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Sparkasse hierdurch ein Schaden entstanden, haften der Konto-/Depotinhaber und die Sparkasse nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung ab der Sperranzeige

Sobald die Sparkasse eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

10a Kündigung des Online-Banking

Das über die 1822direkt für die Sparkasse vermittelte 1822MOBILE-Girokonto ist nur über Online-Banking nutzbar. Kündigt der Teilnehmer als Nutzer einer 1822MOBILE-Girokontos die Vereinbarung über die Teilnahme am Online-Banking, gilt dies zugleich als Kündigung des Girovertrags über das 1822MOBILE-Girokonto mit der Sparkasse.

11 Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Sparkasse kann sich der Konto-/Depotinhaber an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

288123 - 9263/3-3 : 21.06.2019